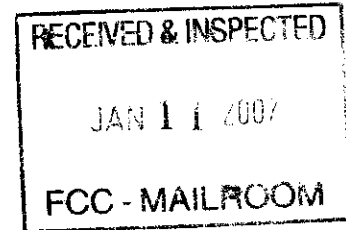


January 10, 2007



Via FedEx Express Overnight Mail
Marlene Dortch, Secretary
Federal Communications Commission
ATTN: Industry Analysis and Technology Division
Wireline Competition Bureau
9300 East Hampton Drive
Capitol Heights, MD 20743



Re: Eschelon Telecom, Inc. Revised CALEA System Security
And Integrity Policies and Procedures Manual
CC Docket 97-213

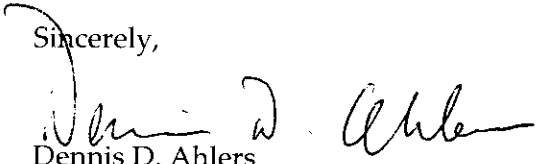
Dear Secretary Dortch:

Pursuant to Section 64.2105 of the Commission's Rules, enclosed are an original and four copies of Eschelon Telecom, Inc.'s revised System Security and Integrity Policies and Procedures Manual with respect to the Communications Assistance for Law Enforcement Act ("CALEA"). This filing revises and updates the information in Eschelon's previous Manual filed with your office on June 9, 2004, as well as the previous Manuals for the Eschelon subsidiaries, including Advanced TelCom, Inc., Mountain Telecommunications Inc., OneEighty Communications, Inc. and Oregon Telecom, Inc. An additional copy of this filing letter is also enclosed. Please date-stamp and return the copy for our records.

The Manual contains sensitive information including the identity and telephone numbers of Eschelon's points of contact. Accordingly, it should be accorded confidential treatment pursuant to Section 0.459 of the Commission's rules and should not be placed in Commission files that are available for inspection by the public.

Please contact me if you have any questions or require additional information.

Sincerely,

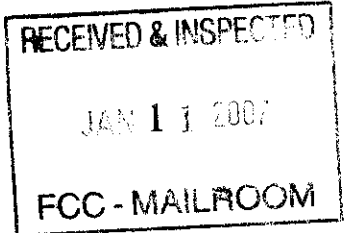

Dennis D. Ahlers
Associate General Counsel
Eschelon Telecom, Inc.
612.436.6249 (direct)
612.436.6349 (fax)
ddahlers@eschelon.com

No. of Copies rec'd 044
List ABCDE

Enclosures

original

Contains Confidential Information



CALEA COMPLIANCE

SYSTEM SECURITY AND INTEGRITY POLICIES AND

PROCEDURES

OF

ESCHELON TELECOM, INC.

including the following subsidiaries:

Advanced TelCom, Inc.
Eschelon Telecom of Arizona, Inc.
Eschelon Telecom of Colorado, Inc.
Eschelon Telecom of Minnesota, Inc.
Eschelon Telecom of Nevada, Inc.
Eschelon Telecom of Oregon, Inc.
Eschelon Telecom of Utah, Inc.
Eschelon Telecom of Washington, Inc.
Mountain Telecommunications, Inc.
OneEighty Communications, Inc., and
Oregon Telecom, Inc.

REVISED January 10, 2007

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. DEFINITIONS.....	2
III. POLICY STATEMENT	3
IV. GENERAL POLICIES AND PROCEDURES FOR EMPLOYEES	3
V. MAINTENACE OF SECURE AND ACCURATE RECORDS.....	4
VI. PRIMARY DESIGNATED EMPLOYEE AND SECONDARY POINTS OF CONTACT .	4
VII. DUTIES OF DESIGNATED EMPLOYEES.	5
APPENDIX A ESCHELON DESIGNATED POINTS OF CONTACT.....	6
APPENDIX B PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE	7
Exhibit 1 - Legal Notification Document	15
APPENDIX C PROCEDURES IF UNAUTHORIZED SURVEILLANCE OR A COMPROMISE OF SURVEILLANCE HAS OCCURRED.....	15
Determination of Record Form.....	16
APPENDIX D CERTIFICATION.....	17
APPENDIX E RELEVANT STATUTES	18
Title 18, Part I	
Title 18, Part II	
Title 50, Chapter 36	

I. INTRODUCTION

This manual contains the updated policies and procedures for Eschelon Telecom, Inc., and each of its operating subsidiary carriers¹ (collectively "Company" or "Eschelon") implementing the Communications Assistance for Law Enforcement Act ("CALEA"). These policies are designed to ensure access by law enforcement officials to authorized wire and electronic communications or call-identifying information² and to ensure that any interception of communications or access to call-identifying information can be activated only in accordance with appropriate legal authorization, appropriate carrier authorization, and with the affirmative intervention of an individual officer or employee of the Company, acting in accordance with Federal Communications Commission ("Commission") regulations. These policies will replace the existing policies on file with the Commission for each of the listed carriers.

These policies and procedures are consistent with the specific requirements found necessary by the Commission as expressed in its Rules and Orders. Among other things, the policies and procedures identify the Primary Designated Employee (as set forth on Appendix A attached hereto) of the Company who is responsible for maintaining such security procedures. These policies and procedures also establish reporting and record-keeping requirements for informing law enforcement officials of all acts of unauthorized Electronic Surveillance that may occur on Company's premises, as well as any other compromises of the carriers' systems security and integrity procedures that involve the execution of Electronic Surveillance.

The purpose of this manual is to make Company employees, including the Designated Employees, aware of Company's policies for compliance with CALEA, Section 229 of the Communications Act and the Commission's rules 47 C.F.R. §§ 1.20000 – 47 C.F.R. 1.20007. The policies and procedures set forth herein are designed to ensure that our employees take only those actions authorized or required by applicable federal and state laws and regulations.

This manual is maintained at the Company's corporate headquarters and at all switching centers of the Company. All relevant employees are required to make themselves familiar with these policies and follow the procedures detailed herein. Designated Employees must sign an annual certification that they have carefully reviewed this manual. If an employee has any questions about any of the information contained herein, the employees should contact the Primary Designated Employee.

¹ The following operating subsidiaries of Eschelon Telecom, Inc. are governed by this Policy Manual: Advanced TelCom, Inc., Mountain Telecommunications, Inc., OneEighty Communications, Inc., Oregon Telecom, Inc., Eschelon Telecom of Arizona, Inc., Eschelon Telecom of Colorado, Inc., Eschelon Telecom of Minnesota, Inc., Eschelon Telecom of Nevada, Inc., Eschelon Telecom of Oregon, Inc., Eschelon Telecom of Utah, Inc., and Eschelon Telecom of Washington, Inc.

² 47 C.F.R. § 64.2103(a).

II. DEFINITIONS

In applying the policies and procedures detailed herein, the Company employees should use the following definitions:

Appropriate Legal Authorization means: (1) a court order signed by a judge or magistrate of competent jurisdiction authorizing or approving interception of wire or electronic communications; or (2) other authorization pursuant to 18 U.S.C. § 2518(7), or any other relevant federal or state statute.

Appropriate Company Authorization means the policies and procedures adopted by the Company to supervise and control officers and employees authorized to assist law enforcement in conducting any interception of communications or access to call-identifying information.

Appropriate Authorization means both Appropriate Legal Authorization and Appropriate Company Authorization.

Company means Eschelon Telecom, Inc. and each of its wholly owned subsidiaries: Advanced Telcom, Inc., Eschelon Telecom of Arizona, Eschelon Telecom of Colorado, Eschelon Telecom of Minnesota, Eschelon Telecom of Oregon, Eschelon Telecom of Nevada, Eschelon Telecom of Utah, Eschelon Telecom of Washington, Mountain Telecommunications, Inc. and Oregon Telecom, Inc.

Designated Employees are those employees authorized by Company to take reasonable actions to comply with valid law enforcement requests for Electronic Surveillance in accordance with the provisions of this manual.

Electronic Surveillance means the implementation of either the interception of the content of a call or the interception of information on the originating or terminating numbers of a call.

Eschelon means Eschelon Telecom, Inc. and each of its wholly owned subsidiaries: Advanced TelCom, Inc., Eschelon Telecom of Arizona, Eschelon Telecom of Colorado, Eschelon Telecom of Minnesota, Eschelon Telecom of Oregon, Eschelon Telecom of Nevada, Eschelon Telecom of Utah, Eschelon Telecom of Washington, Mountain Telecommunications, Inc., OneEighty Communications, Inc. and Oregon Telecom, Inc.

Pen Register is a device that identifies the numbers dialed or otherwise transmitted on the telephone line to Eschelon Telecom of which such device is attached.

Primary Designated Employee is a Designated Employee assigned by the Company with the responsibility for ensuring that Designated Employees of the Company are on call at all times to respond to requests for Electronic Surveillance from law enforcement agencies and for keeping law enforcement agencies informed of changes in Designated Employees and relevant information relating to contacting the Designated Employees. The Primary Designated Employee is also responsible for ensuring that all records required under the provisions of this manual are current and accurate.

Trap and Trace Device is a device that identifies the originating number of an instrument or device from which a wire or electronic communication is transmitted.

III. POLICY STATEMENT

It is the policy of Eschelon Telecom, Inc. to comply with the Communications Assistance for Law Enforcement Act, Public Law No. 103-414, 108 Stat. 4279 (1994) (CALEA), relating to Electronic Surveillance. It is the policy of Eschelon to comply with all federal and state laws and regulations relating to Electronic Surveillance including CALEA. It is the policy of Eschelon to permit only lawful, authorized electronic surveillance to be conducted on its premises. It is also the policy of Company to comply with all relevant record keeping requirements relating to Electronic Surveillance or access to call-identifying information. All employees are required to follow the policies and procedures specified in this document. All personnel must receive Appropriate Legal Authorization and Appropriate Carrier Authorization before enabling law enforcement officials and carrier personnel to implement the interception of communications or access to call-identifying information.

Government agencies do not have the authority to remotely activate interceptions within the switching premises of a telecommunications carrier. Law enforcement personnel may not enter into the Company's property to conduct Electronic Surveillance without the Company's prior knowledge. If any employee becomes aware of any acts of unauthorized Electronic Surveillance on the Company's premises or any compromise or violation of authorized Electronic Surveillance or the policies and procedures contained herein, the employee is required to report the violation to the Primary Designated Employee as soon as possible. Information on the violation shall promptly be documented and a copy of the documentation forwarded by the Primary Designated Employee to the appropriate law enforcement agency.

IV. GENERAL POLICIES AND PROCEDURES FOR EMPLOYEES

Company employees may permit only lawful, authorized Electronic Surveillance to be conducted on Company premises. No Company employee may take any action to initiate or participate in any Electronic Surveillance without Appropriate Authorization.

No employee of the Company may disclose to any person other than relevant law enforcement officials and Designated Employees of the Company, the existence of any interception or surveillance. Employees are advised that discussion with any person other than law enforcement officials and Designated Employees with a need to know (including discussion with family or friends) is strictly prohibited. Unauthorized disclosure of such information constitutes a violation of this policy and a violation of federal and/or state law for which penalties (including immediate termination of employment) may be imposed.

The procedures to be used vary slightly depending upon which statute has been invoked and whether a court order has been obtained. It is important that the Designated Employees follow the specific rules relating to the individual circumstances. Certain Electronic Surveillance is authorized by statute without a court order due to special circumstances in which law enforcement has determined that an emergency situation exists (involving immediate danger of serious physical injury or death, national security or organized crime) and there is insufficient time to obtain a court order. This applies to either call content interception or call information interception using a Pen Register or Trap and Trace Device. In those circumstances, law enforcement officers may seek limited interception of communications absent a court order. However, the requesting law enforcement agency is required to seek court authorization within forty-eight (48) hours of the commencement of the Electronic Surveillance.

V. MAINTENANCE OF SECURE AND ACCURATE RECORDS

The Company shall maintain a secure and accurate record of each interception of communications or access to call-identifying information, made with or without appropriate authorization, in the form of a single Certification, as provided at Appendix D, attached.

Each Certification must include at least the following information, which must be compiled either contemporaneously with, or within a reasonable period of time after the initiation of the interception or the communications or access to call-identifying information:

- A. The telephone number(s) and/or circuit I.D. numbers involved;
- B. The start date and time that the carrier enables the interception of communications or access to call identifying information;
- C. The identity of the law enforcement officer presenting the authorization;
- D. The name of the person signing the appropriate legal authorization;
- E. The type of interception of communications or access to call-identifying information (e.g., pen register, trap and trace, Title III, FISA); and
- F. The name of the telecommunications carriers' personnel who is responsible for overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carriers' policies established under § 1.20003.
- G. The signature of the individual responsible for overseeing the interception of communications or access to call-identifying information and who is acting in accordance with the Company's policies herein, certifying that the Certification is complete and accurate.

The Certification may be completed by appending a copy of the Appropriate Legal Authorization and any extensions that have been granted to the Certification, as long as it contains all of the information in A through F above and the Certification is signed as provided in G above.

Upon completion the Certification shall be placed in the designated confidential, secure Certification file. Eschelon shall maintain and secure these records for a period of no less than twenty-four (24) months.

VI. PRIMARY DESIGNATED EMPLOYEE AND SECONDARY POINTS OF CONTACT

The Company appoints **Gerald Boeke**, Senior Director of Network Operations, or his designee to act as the Primary Designated Employee responsible for ensuring that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the Company. In the event that Eschelon's Primary Contact is unavailable at the time it is necessary for Eschelon to respond to a CALEA request from law enforcement, Eschelon has appointed the employees listed on Exhibit A, attached, as secondary Designated Employees.

Company shall comply by providing the relevant positions and offices, and Central Contact Numbers, which are available 24 hours per day, 7 days a week, as set forth on Appendix A. The Central Contact Numbers are answered/monitored by Company staff, who provide support and supervision for Company's network on a 24/7 basis and which includes an out of hours emergency voice-mail box that is managed at all times. Company will supply the Central Contact Number staff at all times with current telephone numbers and cell phone numbers for

the contact personnel, at least one of which is to be available at all times to receive and respond to requests for services from law enforcement agencies.

Company shall provide the requesting law enforcement agency by facsimile transmission or in electronic form with the form attached at Exhibit 1 to Appendix B, which shall be completed and faxed to Company with appropriate identification and authorization by court order or emergency request before any surveillance service is initiated, to ensure that unauthorized surveillance does not occur.

VII. DUTIES OF DESIGNATED EMPLOYEES.

1. The Designated Employees listed in Appendix A are hereby authorized by Eschelon to implement lawful electronic surveillance in accordance with the policies and procedures in this Manual and to delegate any tasks associated with the surveillance to other employees.
2. Any person designated in Appendix A shall:
 - Oversee the implementation of each electronic surveillance conducted on the premises of Eschelon;
 - Be responsible for ensuring that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of Eschelon.
 - Be responsible for assuring that he/she is fully apprised of all relevant state and federal statutory provisions affecting the legal authorization a carrier must have to conduct electronic surveillance, including section 25 18(7) of Title 18 of the United States Code, which authorizes certain law enforcement personnel to conduct the interception of communications without a court order if an emergency situation exists involving:
 - (i) immediate danger of death or serious physical injury to any person,
 - (ii) conspiratorial activities threatening the national security interest, or
 - (iii) conspiratorial activities characteristic of organized crime.
 - Affirmatively intervene to ensure that there is appropriate legal authorization for each electronic surveillance, including any appropriate authorization required under relevant state and federal statutes;
 - Complete a Certification Form for each electronic surveillance he/she oversees and do so either contemporaneously with, or within a reasonable period of time after the initiation of, the surveillance, so as to develop and maintain a secure and accurate record of each interception of communications or access to call-identifying information made with or without appropriate authorization.
 - Ensure that certification for each surveillance is signed, that the appropriate legal authorization is appended and that it is placed in the appropriate files.

APPENDIX A

ESCHELON DESIGNATED POINTS OF CONTACT

The following Designated Employees are to serve as points of contact for law enforcement agencies. These persons shall be available to law enforcement agencies in such a manner that law enforcement agencies will always be able to contact at least one of them 24 hours a day, 7 days a week.

PRIMARY DESIGNATED EMPLOYEE

Gerald Boeke--Senior Director of Network Operations

Phone: 612-436-6614

Home: 852-544-9518

Cell: 612-251-6630

Fax: 612-335-9494

Pager: 888-249-1340

OTHER DESIGNATED EMPLOYEES

For the following Service Sites:

Santa Rosa, CA (SNRS)

Reno, NV. (RENO)

Salem, OR (SALM)

Tacoma, WA (TACM)

Everett, WA (ERVT)

Yakima, WA (YAKM)

Mike Cavalli--Senior Manager--Switch
Translations, Security & 5ESS Support

Office Phone: 612-436-6032

Cell Phone: 612-336-4527

Fax: 612-436-6132

For the following Service Sites:

Minneapolis, MN (MPLS)

Denver, CO (DNVR)

Portland, OR (PTLD)

Phoenix, AZ (PHNX)

Salt Lake City, UT (SLKC)

Seattle, WA (STTL)

Jon M. Hamer

Manager, Network Translations

Office Phone: 612-436-6652

Cell Phone: 612-281-4417

Fax: 612-436-6752

Pager: 612-319-0649

For Montana and Wyoming Service Sites (BLNG)

Chris Dimock

OEC Management

Office Phone: 406-294-4006

Cell Phone: 406-325-4006

Fax: 406-294-4004

Home: 307-587-7358

APPENDIX B

PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE

I. Call Content Interceptions with a Title III Court Order

- Step One: Any court order presented by a law enforcement agency for a call content interception pursuant to Title III shall be referred immediately to one of the Designated Employees. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears at Exhibit 1 to this Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department.
- Step Two: Before implementing the interception, the Designated Employee shall ensure that the court order contains the following information:
- (a) the identity of the person, if known, whose communications are to be intercepted;
 - (b) the nature and location of the communication facilities or the place for which authority to intercept is granted;
 - (c) a particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates;
 - (d) the period of time during which the interception is authorized, including a statement whether the interception shall automatically terminate when the described communication has been first obtained;
 - (e) a provision that the authorization to intercept shall be executed as soon as practicable and conducted in such a way as to minimize the interception of communications not otherwise subject to interception; AND
 - (f) the signature of a judge or magistrate.
- Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically AND whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implemented, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.
- Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.

APPENDIX B (continued)

- Step Five:** The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order to the Certificate Form and sign the Certification Form. The employee also shall attach to the Certification Form any extensions that are granted for the surveillance.
- Step Six:** The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven:** The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and ensure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the court order (which, in the absence of an extension, cannot exceed 30 days).

II. Call Content Interceptions Pursuant to Title III but without a Court Order

Step One: Any request by a law enforcement agency for a call content interception without a court order, pursuant to the exigent circumstances listed in 18 U.S.C. § 2518(7), shall be referred immediately to one of the Designated Employees. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears as Exhibit 1 to Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department.

Step Two: Before implementing the interception, the Designated Employee shall ensure that the law enforcement agency provides a certification containing the following information:

- (a) the information, facilities, or technical assistance required;
- (b) the period of time during which the provision of information, facilities, or technical assistance is authorized;
- (c) a statement that no warrant or court order is required by law;
- (d) a statement that all statutory requirements have been met;
- (e) a statement that the specific requested assistance is required; AND
- (f) the signature of EITHER (i) the Attorney General of the United States, OR (ii) a law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.

Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically AND whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implement, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.

Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.

APPENDIX B (continued)

Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.

Step Six: The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.

Step Seven: The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and terminate the surveillance as soon as any of the following events occur:

- (a) the law enforcement agency does not apply for a court order within 48 hours after the interception has begun; or
- (b) the law enforcement agency's application for a court order is denied.

Step Eight: If the law enforcement agency receives a court order for the surveillance, the Designated Employee shall validate the court order (as specified in Section I, Step Two above), attach the order to the Certification Form, and handle the surveillance in all respects under the procedures in Section I above.

III. Call Information Interceptions Using a Pen Register or Trap-and-Trace Device with a Court Order

Step One: Any court order presented by a law enforcement agency for a call information interception using a pen register or trap-and-trace device shall be referred immediately to one of the Designated Employees. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears at Exhibit 1 to Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department.

Step Two: Before implementing the interception, the Designated Employee shall determine that the court order contains the following information:

- (a) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap-and-trace device is to be attached;
- (b) the identity, if known, of the person who is the subject of the criminal investigation;
- (c) the number and, if known, physical location of the telephone line to which the pen register or trap-and-trace device is to be attached and, in the case of a trap-and-trace device, the geographical limits of the trap-and-trace order;
- (d) a statement of the offense to which the information likely to be obtained by the pen register or trap-and-trace device relates; AND
- (e) the signature of a judge or magistrate.

APPENDIX B (continued)

- Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically AND whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implement, the Designated Employee will need to complete a Determination Record (attached hereto at Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.
- Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.
- Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order and sign the Certification Form. The employee also shall attach any extensions that are granted for the surveillance.
- Step Six: The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven: The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and ensure that the surveillance terminates when the legal authorization expires. The Designated Employee shall terminate the surveillance at the time specified in the order (which, in the absence of an extension, cannot exceed 60 days).

IV. Call Information Interceptions Using a Pen Register or Trap-and-Trace Device without a Court Order

- Step One One: Any request for a call information interception using a pen register or trap-and-trace device without a court order shall be referred immediately to one of the Designated Employees. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears at Exhibit 1 of Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department.
- Step Two Two: Although the federal statute does not expressly require a certification in these circumstances, the Designated Employee shall ensure that the law enforcement agency provides a certification containing the following information before implementing the request:
- (a) the information, facilities, or technical assistance required;
 - (b) the period of time during which the provision of information, facilities, or technical assistance is authorized;
 - (c) a statement that no warrant or court is required by law;
 - (d) a statement that all statutory requirements have been met;
 - (e) a statement that the specific requested assistance is required; AND

APPENDIX B (continued)

- (f) the signature of a law enforcement officer specially designated by the Attorney General of the United States, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.

- Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically AND whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implement, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.
- Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.
- Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.
- Step Six: The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven: The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and terminate the surveillance as soon as any of the following events occur:
- (a) the information sought is obtained;
 - (b) the law enforcement agency's application for the court order is denies; or
 - (c) 48 hours have lapsed since the installation of the device without the granting of a court order.
- Step Eight: If the law enforcement agency does not receive a court order for the surveillance, the Designated Employee shall validate the court order (as specified in Section I, Step Two above), attach the order to the Certification Form, and handle the surveillance in all respects under the procedures in Section I above.

V. Electronic Surveillance with a Foreign Intelligence Surveillance Act ("FISA") Court Order

- Step One: Any court order presented by a law enforcement agency for Electronic Surveillance pursuant to FISA shall be referred immediately to one of the Designated Employees designated on Appendix A of this manual. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears at Exhibit 1 to Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department.

APPENDIX B (continued)

Step Two: Before implementing the interception, the Designated Employee shall ensure that the court order contains the following information:

- (a) the identity if known, or a description of the target of the Electronic Surveillance;
- (b) the nature and location of each of the facilities or places at which the Electronic Surveillance will be directed;
- (c) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
- (d) the means by which the Electronic Surveillance will be effected and whether physical entry will be used to effect the surveillance;
- (e) the period of time during which the Electronic Surveillance is approved;
- (f) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device;
- (g) a statement directing that the minimization procedures be followed;
- (h) a statement directing that, upon the request of the applicant, a specified carrier furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the Electronic Surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that the carrier is providing that target of Electronic Surveillance;
- (i) a statement directing that the carrier maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain;
- (j) a statement directing that the applicant compensate, at the prevailing rate, the carrier for furnishing the aid; AND
- (k) the signature of a federal district judge.

Whenever the target of the Electronic Surveillance is a foreign power (as defined under FISA) and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the court order need not contain the information required by subparagraphs (c), (d), and (f), but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of Electronic Surveillance involved, including whether physical entry is required.

Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically AND whether the court order is sufficiently and accurately

detailed to enable the carrier to comply with its terms. If the request cannot be implement, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying agency.

Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.

APPENDIX B (continued)

- Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order and sign the Certification Form. The employee also shall attach any extensions that are granted for the surveillance.
- Step Six: The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven: The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and ensure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the order. In the absence of an extension, the surveillance cannot exceed 90 days (or 1 year if the surveillance is targeted against a foreign power).

VI. Electronic Surveillance Conducted Pursuant to FISA but without a Court Order

- Step One: Any request by a law enforcement agency for Electronic Surveillance pursuant to FISA but without a court order shall be referred immediately to one of the Designated Employees on Appendix A. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears at Exhibit 1 to Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department.
- Step Two: Although FISA does not expressly require a certification in these circumstances, the Designated Employee shall ensure that the law enforcement agency provides a certification containing the following information before implementing the request.
- (a) the information, facilities, or technical assistance required;
 - (b) the period of time during which the provision of information, facilities, or technical assistance is authorized;
 - (c) a statement that no warrant or court order is required by law;
 - (d) a statement that all statutory requirements have been met;
 - (e) a statement that the specific requested assistance is required; AND
 - (f) the signature of EITHER (i) the Attorney General of the United States, OR (ii) a law enforcement officer specially designated by the Attorney General.
- Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically AND whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implemented, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.

- Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.
- Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.
- Step Six: The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven: The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and terminate the surveillance as soon as any of the following events occur:
- (a) the information sought is obtained;
 - (b) the law enforcement agency's application for a court order is denied; or
 - (c) 24 hours have elapsed since the authorization of the surveillance by the Attorney General without the granting of a court order.
- Step Eight: If the law enforcement agency does receive a court order for the surveillance, the Designated Employee shall validate the court order (as specified in Section I, Step Two above), attach the order to the Certification Form, and handle the surveillance in all respects under the procedures in Section I above.

APPENDIX B, Exhibit 1

PEN REGISTER, TRAP AND TRACE DEVICE, AND WIRE COMMUNICATIONS INTERCEPTION

LEGAL NOTIFICATION DOCUMENT

A copy of Requestor's identification MUST be attached to this form before commencing Services.

SERVICE TYPE		
<i>Please check all applicable boxes:</i>		
<input type="checkbox"/> Pen Register	<input type="checkbox"/> Emergency Service	<input type="checkbox"/> Non-Emergency Service
<input type="checkbox"/> Trap and Trace Device	<input type="checkbox"/> Emergency Service	<input type="checkbox"/> Non-Emergency Service
<input type="checkbox"/> Wire Communications Interception	<input type="checkbox"/> Emergency Service	<input type="checkbox"/> Non-Emergency Service
<input type="checkbox"/> Court Order <input type="checkbox"/> Other [Please Specify] _____		
<i>Retain a copy of the document and attach The original to this form.</i>		
Commencement Date: _____		Termination Date*: _____
<i>*As specified in the court document, or in the absence thereof, Authorized Requestor's estimated time frame</i>		

Authorized Requestor (*printed name*)

Authorized Requestor (*signature*)

Date

Agency Name

() _____

Phone Number

Superior Name No. 1

() _____

Phone Number

Superior Name No. 2

() _____

Phone Number

Eschelon Designee (*printed name*)

Eschelon Designee (*signature*)

INSTRUCTIONS:

Please notify J. Jeffery Oxley, General Counsel, at 612-436-6692 or Dennis Ahlers, Associate General Counsel at 612-436-6249, as soon as practicable upon completion of this form or for any questions pertaining to the Services. Please contact Catherine A. Murray, Manager, Regulatory Affairs, at 612-436-1632 in the event you are having difficulty locating either Counsel. **Please forward the completed form to Catherine A. Murray, at Eschelon Telecom, Inc., 730 Second Avenue South, Suite 900, Minneapolis, Minnesota 55402.**

APPENDIX C

PROCEDURES IF UNAUTHORIZED SURVEILLANCE OR A COMPROMISE OF SURVEILLANCE HAS OCCURRED

- Step One: If any employee becomes aware of any act of unauthorized Electronic Surveillance or any compromise of authorized surveillance to unauthorized persons or entities, that employee shall report the incident immediately to one of the Designated Employees in Appendix A.
- Step Two: The Designated Employee shall promptly notify Jeffery Oxley, General Counsel or Dennis Ahlers, Associate General Counsel of the incident. Acting with legal counsel, the Designated Employee and Mr. Oxley or Mr. Ahlers shall determine which law enforcement agencies are affected and promptly notify the agencies of the incident.
- Step Three: The Designated Employee shall compile a certification record for any unauthorized surveillance and ensure that all records available to the carrier regarding the surveillance are placed in the appropriate carrier files. If the request cannot be implemented, the Designated Employee will need to complete a Determination Record (attached hereto), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.

APPENDIX C (continued)

DETERMINATION OF RECORD

The undersigned, an employee designated by the Company to respond to and oversee the implementation of legal Electronic Surveillance requests from law enforcement agencies hereby certifies that the Company cannot implement the requested Electronic Surveillance for the reason(s) noted below:

A. Telephone number(s) and/or circuit identification numbers

involved: _____

B. Requested start date (including date and time): _____

C. Name of person signing the Appropriate Legal Authorization: _____

D. The type of interception of communications or access to call-identifying information (e.g., Pen Register, Trap and Trace Device): _____

E. Reason that the interception of communications or access to call-identifying information cannot technically be provided (e.g. technical inability: customer of different carrier):

F. Name of the Company's personnel responsible for overseeing the interception of communication or access to call-identifying information and signing this form:

Signature

Date

Phone No.

APPENDIX D
CERTIFICATION

The undersigned, Designated Employee, hereby certifies that this is a true and complete record of the information received and actions taken relative to the attached Appropriate Legal Authorization. The undersigned further certifies that on the date and time indicated below appropriate actions were taken to implement the Electronic Surveillance referenced in the attached court order or other Legal Authorization relating to the following:

A. Telephone number(s) and/or circuit identification numbers involved: _____

B. Start date (including date and time) of the circuit opening for law enforcement: _____

D. Name of person signing the Appropriate Legal Authorization: _____

E. The type of interception of communications or access to call-identifying information:

1. pen register

2. trap and trace

3. Title III,

4. FISA

5. Other (explain) _____

F. The date that the interception is scheduled to be terminated: _____

G. Date of actual termination: _____

By my signature, I certify that I am duly authorized by the Company and am responsible for overseeing the interception of communication or access to call-identifying information and that I have overseen the interception of communications or access to call-identifying information described above and that this Certification is complete and accurate.

Printed Name: _____

Signature: _____

Date: _____

T:\Legal\CALEA\ATI CALEA Manual-Esch draft.doc

TITLE 18--CRIMES AND CRIMINAL PROCEDURE

PART I--CRIMES

CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND
INTERCEPTION OF ORAL COMMUNICATIONS

Sec. 2510. Definitions

As used in this chapter--

(1) ``wire communication'' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) ``oral communication'' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) ``State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) ``intercept'' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.\1\

\1\ So in original. The period probably should be a semicolon.

(5) ``electronic, mechanical, or other device'' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) ``person'' means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) ``Investigative or law enforcement officer'' means any

officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) ``contents'', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) ``Judge of competent jurisdiction'' means--

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) ``communication common carrier'' has the meaning given that term in section 3 of the Communications Act of 1934;

(11) ``aggrieved person'' means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) ``electronic communication'' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) ``user'' means any person or entity who--

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) ``electronic communications system'' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) ``electronic communication service'' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) ``readily accessible to the general public'' means, with respect to a radio communication, that such communication is not--

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a

common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) ``electronic storage'' means--

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) ``aural transfer'' means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) ``foreign intelligence information'', for purposes of section 2517(6) of this title, means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) ``protected computer'' has the meaning set forth in section 1030; and

(21) ``computer trespasser''--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

TITLE 18--CRIMES AND CRIMINAL PROCEDURE

PART I--CRIMES

CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND
INTERCEPTION OF ORAL COMMUNICATIONS

Sec. 2511. Interception and disclosure of wire, oral, or
electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any
person who--

(a) intentionally intercepts, endeavors to intercept, or
procures any other person to intercept or endeavor to intercept, any
wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other
person to use or endeavor to use any electronic, mechanical, or
other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a
signal through, a wire, cable, or other like connection used in
wire communication; or

(ii) such device transmits communications by radio, or
interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such
device or any component thereof has been sent through the mail
or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the
premises of any business or other commercial establishment the
operations of which affect interstate or foreign commerce; or
(B) obtains or is for the purpose of obtaining information
relating to the operations of any business or other commercial
establishment the operations of which affect interstate or
foreign commerce; or

(v) such person acts in the District of Columbia, the
Commonwealth of Puerto Rico, or any territory or possession of
the United States;

(c) intentionally discloses, or endeavors to disclose, to any
other person the contents of any wire, oral, or electronic
communication, knowing or having reason to know that the information
was obtained through the interception of a wire, oral, or electronic
communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any
wire, oral, or electronic communication, knowing or having reason to
know that the information was obtained through the interception of a
wire, oral, or electronic communication in violation of this
subsection; or

(e)(i) intentionally discloses, or endeavors to disclose, to any
other person the contents of any wire, oral, or electronic
communication, intercepted by means authorized by sections
2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this
chapter, (ii) knowing or having reason to know that the information
was obtained through the interception of such a communication in
connection with a criminal investigation, (iii) having obtained or
received the information in connection with a criminal
investigation, and (iv) with intent to improperly obstruct, impede,